

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

VITALII ANTONENKO,
a/k/a “Sabe,”
a/k/a “Sabeseller”

Defendant

) Criminal No. 20-10102
)

) Violations:
)

) Count One: Conspiracy to Gain Unauthorized
) Access and to Traffic in Unauthorized Access
) Devices

) (18 U.S.C. § 371)
)

) Count Two: Money Laundering Conspiracy
) (18 U.S.C. § 1956(h))
)

) Forfeiture:
)

) (18 U.S.C. §§ 981(a)(1)(C), 982(a)(1) &
) 28 U.S.C. § 2461)
)

INDICTMENT

At all times relevant to this Indictment:

General Allegations

1. Defendant Vitalii Antonenko, a native of Ukraine, resided in New York City.
2. Coconspirator 1 (“CC1”), a coconspirator not charged as a defendant in this Indictment, resided in New York City and Ukraine.
3. Coconspirator 2 (“CC2”), a coconspirator not charged as a defendant in this Indictment, resided in Russia and one of the former Soviet Republics.
4. CC2 operated “Carding Forum A.” Since at least as early as 2012, Carding Forum A was a website that offered for sale the personally identifiable information (“PII”) of hundreds of millions of consumers throughout the United States and around the world. Such PII included names, dates of birth, Social Security Numbers, and payment card data, including credit and

debit card account numbers, expiration dates, and card verification values (“Payment Card Data”).

5. Coconspirator 3 (“CC3”), a coconspirator not charged as a defendant in this Indictment, resided in or near Los Angeles, California. CC3 ran an unlicensed business that exchanged Bitcoin, a digital currency, for cash, and cash for Bitcoin.

6. Victim 1 was a hospitality business headquartered in eastern Massachusetts.

7. Victim 2 was a non-profit, scientific research institution located in eastern Massachusetts.

8. A “SQL Injection Attack” was a series of computer commands that could be used to gain unauthorized access to computer networks that store data, including Payment Card Data and other PII.

9. A “Shell” is a kind of malicious software that an intruder can install on a victim computer network. A Shell can enable an intruder easy return access to the victim computer network and the ability to control it remotely.

Object and Purpose of the Hacking-Carding Conspiracy

10. The objects of the conspiracy charged in Count 1 of this Indictment (“the Hacking-Carding Conspiracy”) were for defendant Vitalii Antonenko, CC1, CC2, and others known and unknown to the Grand Jury to:

- a. access computer networks without authorization, in order to obtain PII, including Payment Card Data, hosted on those networks, in violation of 18 U.S.C. §§ 1030(a)(2)(C); and
- b. sell the PII, including Payment Card Data, over Carding Forum A and

other criminal carding forums, in violation of 18 U.S.C. § 1029(a)(2).

11. It was the purpose of the conspiracy to profit from unauthorized access to computer networks and to conceal the coconspirators' actions from law enforcement.

Manner and Means of the Hacking-Carding Conspiracy

12. Among the manner and means by which Antonenko, a/k/a "Sabe," a/k/a "Sabeseller," CC1, CC2, and coconspirators known and unknown to the Grand Jury carried out the conspiracy were the following:

a. scouring the internet and searching for computer networks with security vulnerabilities that would permit the members of the conspiracy to obtain unauthorized access to networks that were likely to hold PII, including Payment Card Data, or to usernames and passwords that would permit access to PII, including Payment Card Data;

b. exploiting the vulnerabilities using various hacking techniques and tools, including SQL Injection Attacks and Shells;

c. obtaining unauthorized access through Virtual Private Networks that disguised the coconspirators' true locations;

d. identifying and extracting Payment Card Data and other PII from the victims' networks;

e. consigning Payment Card Data and other PII for sale over Carding Forum A; and

f. sharing in Bitcoin proceeds of any sales that took place.

Overt Acts in Furtherance of the Hacking-Carding Conspiracy

13. From in or about December 2013 through in on about November 2016, Antonenko,

a/k/a “Sabe,” a/k/a “Sabeseller,” CC1, CC2, and coconspirators known and unknown to the Grand Jury committed and caused to be committed the following overt acts, among others, in furtherance of the conspiracy:

Overt Acts Relating to Victim 1

a. On or about December 18, 2013, Antonenko obtained access to the email account of a computer network administrator at Victim 1.

b. On or about December 20, 2013, Antonenko messaged a coconspirator that he had located more than 2.8 million pieces of Payment Card Data within Victim 1’s computer network.

c. On or about March 17, 2014, Antonenko messaged a potential customer for Payment Card Data, “I’m a hacker[.] Hack nonstop[.] I’m the top guy in other shops[.] Upload up to 50k-100k. Do you know [Carding Forum A]? I give them 40k a day[.] I support them well[.]”

d. On or about August 3, 2014, Antonenko messaged a coconspirator that he had escalated his access privileges within Victim 1’s computer network and was looking for Payment Card Data.

e. On or about August 4, 2014, Antonenko messaged a coconspirator that he controlled shell access to Victim 1’s computer network and would attempt to obtain Payment Card Data.

f. On or about August 4, 2014, Antonenko accessed Victim 1’s computer network and installed Shells and other malware to manage the coconspirators’ remote access to the network and to obtain Payment Card Data.

g. On or about August 12, 2014, Antonenko messaged a coconspirator that he had obtained 4.5 million pieces of Payment Card Data (without card verification values) from Victim 1's computer network.

h. On or about August 16, 2014, Antonenko attempted to access Victim 1's computer network from an IP address owned by Internet Service Provider 1 ("ISP 1") that was then assigned to the New York City apartment building where Antonenko was living.

i. On August 26, 2014, a coconspirator sent Antonenko an inventory of credit cards for sale on Carding Forum A indicating that Antonenko's account had 73,000 payment cards offered for sale.

j. On September 26, 2014, responding to news coverage about the data breach at Victim 1, Antonenko messaged a coconspirator that he was nervous about the mention of ISP 1 as a possible vector for the attack, because Antonenko had used ISP 1 when his Virtual Private Network was not stable. In response, the coconspirator suggested to Antonenko that he move away from his apartment.

k. On May 5, 2015, Antonenko sent CC2 a message requesting "1.5k" related to Victim 1 and provided a Bitcoin address.

l. On May 5, 2015, CC2 sent Antonenko an accounting of the number of Payment Cards that Antonenko had sold over Carding Forum A (approximately 109,000) and the amount that Carding Forum A owed Antonenko (\$1,063.53).

m. On May 5, 2015, Antonenko sent CC2 a message stating that he still had "200k" more pieces of Payment Card Data "from [Victim 1]" that he could send to Carding Forum A for sale.

n. On May 5, 2015, CC2 sent Antonenko 4.38 Bitcoin (then worth approximately \$1,035.83) to a Bitcoin wallet that Antonenko controlled.

o. On October 27, 2015, Antonenko messaged a coconspirator that he still had unauthorized access to Victim 1's network.

p. On or about November 4, 2016, CC2 sold Payment Card Data over Carding Forum A to an undercover law enforcement officer in Massachusetts, including the Payment Card Data of a customer of Victim 1 who lived in Massachusetts.

Overt Acts Relating to Victim 2

q. On or about July 13, 2015, Antonenko messaged a coconspirator the results of an effort to map portions of Victim 2's network that were vulnerable to SQL Injection Attacks.

r. On or about July 28, 2015, Antonenko messaged a coconspirator two internet links providing access to Victim 2's network.

s. On or about July 28, 2015, Antonenko obtained information stored in databases on Victim 2's network and saved that information to a storage device that he controlled.

Object and Purpose of the Money Laundering Conspiracy

14. It was the object and purpose of the Money Laundering Conspiracy charged in Count 2 of this Indictment to use cash, bank account, and cryptocurrency transactions to conceal the nature, location, source, ownership, and control of the proceeds of the Hacking-Carding Conspiracy.

Manner and Means of the Money Laundering Conspiracy

15. Among the manner and means by which Vitali Antonenko, a/k/a "Sabe," a/k/a "Sabeseller," CC2, CC3, and coconspirators known and unknown to the Grand Jury carried out

the Money Laundering Conspiracy were the following:

- a. CC2 and other coconspirators transferred Bitcoin representing the proceeds from the sale of Payment Card Data and other PII to Bitcoin wallets that Antonenko controlled.
- b. Antonenko transferred the Bitcoin that he received from CC2 and others to Bitcoin wallets that CC3 controlled.
- c. CC3 either met with Antonenko in person and gave him cash or deposited cash into bank accounts that Antonenko controlled.
- d. CC3 sometimes split deposits across multiple branches of the same bank or structured deposits.
- e. CC3 paid Antonenko approximately 10 percent less than prevailing market rates for the Bitcoin that Antonenko sold to CC3.

Acts in Furtherance of the Money Laundering Conspiracy

16. Between in or about January 2014 through at least January 2016, Vitalii Antonenko, a/k/a “Sabe,” a/k/a “Sabeseller,” CC2, CC3, and coconspirators known and unknown to the Grand Jury committed and caused to be committed the following acts, among others, in furtherance of the conspiracy:

- a. On or about the dates below, CC2 sent the Bitcoin amounts in the values below to wallets that Antonenko controlled; Antonenko sent the amounts below to a wallet that CC3 controlled; and CC3 then caused deposits to be made in bank accounts that Antonenko controlled.

DATE	CC2 to Antonenko	Antonenko to CC3	CC3 to Antonenko
03/30/14	25 BTC		
4/1/14	--	24.9999 BTC	\$9,900 \$1,133
4/11/14	26.25 BTC (\$10,579.28)	26.2 BTC	\$9,609
5/20/14	8.65 BTC (\$4,018.10)	8.5 BTC	\$3,790
7/5/14	4 BTC (\$2,669.41)	4 BTC	\$2,290
12/16/14	6.2 BTC (\$2,089.79)	6.17 BTC	\$1,870
12/26/14	6.2 BTC (\$2,008.86)	6.17 BTC	\$1,814
1/8/15	7.17 BTC (\$2,073.56)	7.17 BTC	\$1,902
3/9/15	3.63 BTC (\$1,025.66)	3.7 BTC	\$953
4/20/15	4.88 BTC (\$1,096.54)	4.77717 BTC	\$975
5/5/15	4.38 BTC (\$1,035.83)	3.717 BTC	\$795
5/28/15	7.79 BTC (\$1,858.23)	7.7717 BTC	\$1,357
6/8/15	10.38 BTC (\$2,353.87)	11.17 BTC	\$2,320

COUNT ONE
Hacking-Carding Conspiracy
(18 U.S.C. § 371)

The Grand Jury charges:

17. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 16 of this Indictment.

18. Between in or about December 2013 and in or about November 2016, in the District of Massachusetts, and elsewhere, the defendant,

VITALII ANTONENKO,
a/k/a "Sabe,"
a/k/a "Sabeseller"

conspired with CC1, CC2, and with others known and unknown to the Grand Jury to commit the following offenses:

a. Unauthorized access to computers, that is, to intentionally access a computer without authorization and thereby obtain information from any protected computer, and knowingly, and with intent to defraud, access a protected computer without authorization, and by means of such conduct further the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (a)(4), (c)(2)(B), and (c)(3); and

b. Access device fraud, that is, to knowingly, and with intent to defraud, traffic in and use one or more unauthorized access devices, namely credit and debit card account numbers, credit and debit card account expiration dates, credit and debit card verification values, and Social Security Numbers, during any one-year period, and by such conduct obtain anything of value aggregating \$1,000 or more during that period, in violation of Title 18, United States Code, Section 1029(a)(2).

All in violation of Title 18, United States Code, Section 371.

COUNT TWO

Money Laundering Conspiracy
(18 U.S.C. § 1956(h))

19. The United States Attorney re-alleges and incorporates by reference paragraphs 1 through 16 of this Indictment.

20. From in or about January 2014 through on or about June 8, 2015, in the District of Massachusetts, and elsewhere, the defendant,

Vitalii Antonenko,
a/k/a "Sabe,"
a/k/a "Sabeseller,"

did conspire with CC2, CC3 and others known and unknown to the Grand Jury to conduct and attempt to conduct financial transactions, to wit, Bitcoin-for-cash exchanges, knowing that the property involved in such transaction represented the proceeds of some form of unlawful activity, and which in fact involved the proceeds of specified unlawful activity, that is, unauthorized access to protected computers and trafficking in PII, including Payment Card Data, and knowing that the transactions were designed, in whole and in part, to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

All in violation of Title 18, United States Code, Section 1956(h).

CONSPIRACY FORFEITURE ALLEGATION

(18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c))

1. Upon conviction of the offense in violation of Title 18, United States Code, Section 371, set forth in Count One, the defendant,

Vitalii Antonenko,
a/k/a “Sabe,”
a/k/a “Sabeseller,”

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense.

2. If any of the property described in Paragraph 1, above, as being forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), as a result of any act or omission of the defendant –

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the property described in Paragraph 1 above.

All pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c).

MONEY LAUNDERING FORFEITURE ALLEGATION

(18 U.S.C. § 982(a)(1))

1. Upon conviction of the offense in violation of Title 18, United States Code, Section 1956, set forth in Count Two, the defendant,

Vitalii Antonenko,
a/k/a "Sabe,"
a/k/a "Sabeseller,"

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in such offense, and any property traceable to such property.

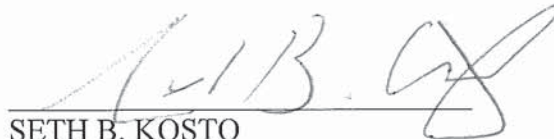
2. If any of the property described in Paragraph 1, above, as being forfeitable pursuant to Title 18, United States Code, Section 982(a)(1), as a result of any act or omission of the defendant –

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to Title 18, United States Code, Section 982(b), incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the property described in Paragraph 1 above.

All pursuant to Title 18, United States Code, Section 982(a)(1).

A TRUE BILL


FOREPERSON
SETH B. KOSTO
ASSISTANT UNITED STATES ATTORNEY
DISTRICT OF MASSACHUSETTS

District of Massachusetts: May 26, 2020
Returned into the District Court by the Grand Jurors and filed.

/s/ Lisa Belpedio, 3:52 p.m.
DEPUTY CLERK